

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X

Joint Stock Company “Channel One Russia Worldwide,”  
Closed Joint Stock Company “CTC Network,” Closed  
Joint Stock Company “TV DARIAL,” Closed Joint  
Stock Company “New Channel,” Limited Liability  
Company “Rain TV-Channel,” and Limited Liability Company  
“Comedy TV.”

Index No. 16-cv-1318  
(GBD)(BCM)

Plaintiffs,

-against-

**FIRST AMENDED  
VERIFIED COMPLAINT**

INFOMIR LLC ( [www.infomirusa.com](http://www.infomirusa.com)), INFOMIR GMBH,  
ALEXANDER MARAHOVSKY, EVGENI LEVITIN,  
TELECOMMUNICATIONS TECHNOLOGIES LTD.,  
PANORAMA ALLIANCE, LP ([www.mypanorama.tv](http://www.mypanorama.tv)),  
ASAF YEVDAYEV, DAVID ZELTSER,  
GOODZONE TV ([www.gudzon.tv](http://www.gudzon.tv)),  
MOIDOM LLC, TELEPROM, VDALI, MHCOM GmbH and  
John Does 1-50.

Defendants.

-----X

Plaintiffs Joint Stock Company “Channel One Russia Worldwide” (“Channel One”),  
Closed Joint Stock Company “CTC Network” (“CTC”), Closed Joint Stock Company “TV  
DARIAL” (“DARIAL”), Closed Joint Stock Company “New Channel” (“New Channel”),  
Limited Liability Company “Rain TV-Channel” (“Rain TV”), and Limited Liability Company  
“Comedy TV” (“Comedy TV”) (each a “Plaintiff” or collectively “Broadcasters”),<sup>1</sup> by their  
attorneys, Dunnington Bartholow & Miller LLP (“Dunnington”), as and for their First Amended  
Verified Complaint against Defendants Infomir LLC (“Infomir”), Infomir GmbH, Alexander  
Marahovsky (“Marahovsky”), Evgeni Levitin (“Levitin”), Telecommunications Technology Ltd.  
 (“Teletec”) (together “the Infomir Defendants”), Panorama Alliance, LP (“Panorama”),

---

<sup>1</sup> A reference to a Plaintiff or Plaintiffs shall be deemed to include its or their parents, subsidiaries, licensees and affiliates.

Goodzone TV a/k/a Gudzon TV (“Goodzone”), Asaf Yevdayev (“Yevdayev”), David Zeltser a/k/a Zeltzer (“Zeltser”), Moidom (“Moidom”), Vdali (“Vdali”), MHCOM GmbH (“Mhcom”), and John Does 1-50 (each of the foregoing a “Defendant” and collectively “Defendants”) for violations of the Federal Communications Act, the Copyright Act, the Lanham Act trademark, and claims under the New York General Business Law and aver as follows:

### **PRELIMINARY STATEMENT**

1. Defendants provide video streaming services of Russian-language television channels to paying subscribers throughout the United States without the authority of the Broadcasters who own the channels. Using an unauthorized method as yet unknown to Broadcasters, Defendants intercept Broadcasters’ encrypted foreign satellite transmissions, transform the transmissions into digital data, then re-transmit the channels over the internet to paying subscribers in the U.S. using password-protected streaming services. In addition to the foregoing, three Defendants, Infomir LLC, Infomir GmbH, and Telecommunications Technology LTD controlled by their principals, Marahovsky & Levitin (the “Infomir Defendants”), also manufacture and sell set-top boxes which are configured and marketed to facilitate piracy and over which the Infomir Defendants maintain control through software that is specifically designed to promote and exploit piracy of Broadcasters’ channels. The Infomir Defendants also sell a version of the set top boxes sold with pre-loaded software “apps” that permit subscribers to launch browsers from the set-top boxes permitting subscribers to view Broadcasters’ channels over streaming services. The Infomir Defendants actively promote piracy of Broadcasters’ programming by selling set-top boxes, servers and software to known infringers and providing instructions to software that facilitates large-scale commercial piracy. The Infomir Defendants fail to take reasonable antipiracy security measures in manufacturing the device and in distributing software consistent with industry standards, such as https security,

blacklisting and extended validation certificates or implementing other industry-standard antipiracy measures. This failure, combined with Infomir-designed “Stalker middleware” converts the set-top boxes into circumvention tools to promote piracy by others, ensuring that the primary use of the set-top boxes is for piracy of Broadcasters’ copyright-protected content. Although Infomir Defendants could block known pirates from using the set-top boxes by simply updating the firmware that runs the boxes, the Infomir Defendants refuse to do so. Thus, the Infomir Defendants both operate a pirate streaming service *and* manufacture and sell equipment and software designed to assist and profit from other pirates, essentially a “piracy startup kit.”

2. Because each Defendant either directly intercepts Broadcasters’ satellite communications or knowingly re-transmits intercepted satellite communications, each Defendant’s conduct violates the Federal Communications Act of 1934, 47 U.S.C. §605 (“the FCA”). Because each Defendant unlawfully and knowingly copies content protected by the Copyright Act and the Lanham Act, each Defendant’s conduct violates the provisions of those statutes forbidding copyright and trademark infringement. Because each Defendant bypasses the Broadcasters’ encryption or retransmits de-encrypted copyrighted content, each Defendants’ conduct violates the anti-circumvention measures of the Digital Millennium Copyright Act (“DMCA”) 17 U.S.C. §102 et seq. Because the Infomir Defendants manufacture, import and distribute devices and provide Stalker middleware that, together, are primarily of assistance in the unauthorized decryption of satellite cable programming, the Infomir Defendants have violated additional provisions of the FCA that forbid trafficking in devices that permit circumvention tools, 47 U.S.C. §604(e)(4) and the DMCA 17 U.S.C. §1201(a)(2) which prohibits the manufacture and import of technology that “is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title...” 17 U.S.C.A. § 1201.

3. Each of the Broadcasters has an established, famous trademark or trademarks in the United States and international versions of their Russian-language channels are known to a loyal fan base of cable, satellite and IPTV subscribers in the United States distributed through reputable distributors, including Time Warner Cable, Directv, Optimum and Xfinity.

4. Defendants are conducting and promoting piracy of Broadcasters' content on a large systematic, commercial scale that demonstrates willfulness, warranting the severest imposition of damages warranted by law. Each of the Broadcasters has suffered and continues to suffer economic loss in the United States due to Defendants' provision of pirated versions of their channels. Additionally, each Broadcaster is put at reputational risk by continued piracy because the Defendants' pirated versions of the channels contain programming that is licensed for foreign broadcasts only, not for the U.S. Thus, the sales and markets for fully-licensed international versions in the United States of Broadcasters' channels are unfairly undercut and irreparably harmed by Defendants' piracy and unfair competition. Such piracy irreparably harms the reputation of the Broadcasters with the licensors of such content.

5. Because the Broadcasters do not know exactly how Defendants intercept satellite communications and cannot presently state whether and to what extent additional persons are involved in the interception, data conversion, and resales process leading to the illegal streams identified herein, John Does 1-50 are named. Because the evidence of how Broadcasters' satellite communications are intercepted and distributed is in the possession of Defendants or Defendants' John Doe agents or accomplices, Broadcasters are unable to plead additional facts or identify additional infringers until discovery is had. Broadcasters expect that certain John Does will be corporations that transmit large amounts of data traffic over the internet. Through these proceedings, Broadcasters seek to identify and block all such infringing transmissions.

## **THE PARTIES**

### **A. Plaintiffs**

6. Plaintiff Channel One is a joint stock company located in and organized under the laws of the Russian Federation with its headquarters located at 19 Akademika Koroleva St. Moscow, 127427 Russian Federation. Channel One produces, among others, “Channel One.” The Channel One logo is:



Channel One’s television channels have the largest audience in the Russian Federation and the Commonwealth of Independent States (“CIS.”) Channel One broadcasts a wide range of news, documentary and feature film productions, as well as entertainment programs that attract a greater number of viewers each year. Among the other channels produced by Channel One are a European and U.S. version of Channel One Russia Worldwide, Dom Kino, Muzika Pervogo, Vremya:dalekoe i blizkoe, Carousel International, and Telekafe. Additionally, Channel One is authorized by its parent corporation to represent its interests relating to unauthorized distribution of the Russian version of Channel One Russia.

7. The logo of the Dom Kino channel is:



8. The logo of the Carousel International channel is:



9. The logo of the Muzika Pervogo channel is:



10. The logo of the Telekafe channel is:



11. The logo of the Vremya:dalekoe i blizkoe channel is:



12. Channel One has entered into license agreements with one or more third parties to distribute its programs via IPTV in the United States. Because Channel One is obligated to charge at least as much for its programming to any third party pursuant to a “most favored nation” clause, Defendants’ actions cause Channel One immediate and irreparable harm because the efforts of its licenses to attract subscribers have been undercut by pirates offering lower prices.

13. Channel One’s established, famous trademarks in the United States and international versions of its Russian-language channels are known to a loyal fan base in the United States and are distributed through reputable distributors, including Time Warner Cable, Directv, Optimum and Xfinity. Attached hereto as **Exhibit 1** is a screenshot of the Time Warner

Cable advertising Channel One in the United States. Attached hereto as **Exhibit 2** is a screenshot of the Directv website advertising Channel One in the United States. Attached hereto as **Exhibit 3** is a screenshot of the Optimum website advertising Channel One in the United States. Attached hereto as **Exhibit 4** is a screenshot of the Xfinity website advertising Channel One in the United States.

14. Defendants are not authorized to broadcast Channel One, Dom Kino, Carousel International, Muzika Pervogo, Telekafé, or Vremya:dalekoe i blizkoe in the United States or elsewhere.

15. Plaintiff CTC is a closed joint stock company located in and organized under the laws of the Russian Federation. CTC produces the CTC channel. The CTC channel logo is:



The CTC channel has been broadcasting continuously since 1996 and features Russian and foreign programming, including but not limited to dramas, sitcoms, humor, music and general entertainment shows and advertising.

16. CTC has entered into license agreements with third parties to distribute its programs via IPTV in the United States and around the world.

17. CTC's established, famous trademark in the United States is known to a loyal fan base in the United States. International versions of its Russian language channel are distributed by reputable distributors such as Time Warner Cable and Optimum. (See **Exhibits 1 & 3**)

18. Defendants are not authorized to broadcast the CTC channel in the United States or elsewhere.

19. Plaintiff Darial is a closed joint stock company located in and organized under the laws of the Russian Federation. Darial produces the Che TV channel and previously produced the Peretz channel. The Che TV channel logo is:



20. Darial has entered into exclusive license agreements with third parties to distribute its programs via IPTV in the United States and around the world. Defendants are not authorized to broadcast the Che TV channel in the United States or elsewhere.

21. Plaintiff New Channel is a closed joint stock company located in and organized under the laws of the Russian Federation. New Channel produces the Domashny channel. The Domashny channel logo is:



The Domashny channel began broadcasting in 2005 and is a specialized Russian language thematic channel that targets a female audience.

22. New Channel has entered into license agreements with third parties to distribute its programs via IPTV in the United States and around the world. Defendants are not authorized to broadcast the Domashny channel in the United States or elsewhere.

23. Plaintiff Comedy TV is a limited liability company located at 129301, Moscow, 10 Troitskaya Str., Building 2 and organized under the laws of the Russian Federation. Comedy TV produces the TNT-Comedy Channel. The TNT-Comedy Channel Logo is:



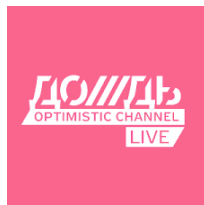
TNT-Comedy Channel is an international version of the Russian TNT TV channel created for the Russian-speaking population living outside the Russian Federation, as well as Russian and Russian-speaking tourists worldwide.

24. Comedy TV has entered into license agreements with third parties to distribute its programs via IPTV in the United States and around the world.

25. Defendants are not authorized to broadcast TNT-Comedy Channel in the United States or elsewhere.

26. Plaintiff Rain TV-Channel is a limited liability company located at 127015, Moscow ul. Bolshaya Novodmitrovskaya 36, str 2 and organized under the laws of the Russian Federation.

27. The Rain TV-Channel Logo is:



Rain TV focuses on news, discussions, culture, politics, business reports, and documentaries.

28. Rain TV has entered into exclusive license agreements with third parties to distribute its programs via IPTV in the United States and around the world.

29. Defendants are not authorized to broadcast Rain TV's channel in the United States or elsewhere.

**B. Defendants**

30. Defendant Infomir is an entity organized and existing under the laws of the State of New York with a principal place of business located at 2469 65 St, STE B4 Brooklyn, NY 11204 USA. Annexed hereto as **Exhibit 5** is the Entity Information concerning Infomir LLC maintained by the New York Secretary of State. Upon information and belief, Infomir owns and operates the websites www.infomirusa.com, infomir.eu and www.infomir.us.

31. Upon information and belief, Infomir is affiliated with defendant Infomir GmbH, a German corporation that has its principal place of business at 56 Kaiserstrasse, Frankfurt Germany, 60329.

32. Upon information and belief, Infomir is affiliated with defendant Teletec, a Ukrainian entity that has its principal place of business at 1 Mytna Square, Odessa, 65026, Ukraine.

33. Upon information and belief, Defendant Alexander Marahovsky is one of two managing directors of Infomir GmbH and owns and controls Teletec.

34. Upon information and belief, Defendant Evgeni Levitin is one of two managing directors of Infomir GmbH. Both Marahovsky and Levitin directly promote and oversee Infomir GmbH's infringement and appropriation of the Programming.

35. Upon information and belief Teletec manufactures the AURA and MAG set-top boxes for Infomir GMBH. Attached hereto as **Exhibit 6** is an image of the packaging of an Aura HD set-top box including the information that the box is "Manufactured by: Telecommunication Technologies" and "Manufactured for Infomir GMBH."

36. Upon information and belief, the Infomir Defendants are manufacturing, importing and selling receivers or “set-top boxes” that are designed primarily to facilitate U.S. subscribers of Infomir and others to receive versions of the Programming that have been intercepted from satellite communications without authorization.

37. Upon information and belief, the Infomir Defendants design Stalker middleware and servers that are primarily designed to assist large scale infringers in re-transmitting unauthorized satellite communications to U.S. consumers by providing a means by which infringers can issue passwords, bill consumers, and provide access to streamed content to set-top boxes sold by Infomir.

38. Upon information and belief, the Infomir Defendants designed the Stalker middleware to efficiently put Broadcasters’ content behind a paywall and to bill for it on a large commercial scale, primarily to assist in circumventing Broadcasters’ technological measures that effectively control access to the Programming and to enable each infringer to profit from hundreds or thousands of subscribers, with each pirate essentially becoming its own Netflix-type service, using content stolen from Broadcasters.

39. Upon information and belief, Panorama is a UK limited partnership that maintains a principal place of business located at 1702 Ave Z, Second Floor, Brooklyn, NY 11235. Panorama owns and operates the domain [www.mypanorama.tv](http://www.mypanorama.tv) which provides unauthorized access to video streams of pirated version of the Programming. Panorama is in active concert and participation with Asaf Yevdayev, who is listed as the original and current registrant of the domain name mypanorama.tv.

40. Defendants David Zeltser a/k/a Zeltzer and Asaf Yevdayev are either officers or directors, or operate as such *de facto* or otherwise control Panorama. Both Zeltser and Yevdayev

are promoting, directing and profiting from the infringement and appropriation of the Programming.

41. Defendant Yevdayev is a resident of Brooklyn, New York and maintains a place of business at 1702 Ave Z, Second Floor, Brooklyn, NY 11235.

42. Defendant Yevdayev is involved in the day-to-day operation of Panorama in Brooklyn, filling subscriptions for its illegal service, answering technical support questions, and processing payments. Defendant Yevdayev is the registrant and current owner of the domain name [www.mypanorama.tv](http://www.mypanorama.tv). Defendant Yevdayev is promoting, directing and profiting from the infringements and other violations of Panorama identified below.

43. Defendant David Zeltser is, on information and belief, a resident of the United Kingdom. Defendant Zeltser is, on information and belief, an officer or director, or otherwise in control of Panorama. Defendant Zeltser is promoting, directing and profiting from the infringements and other violations of Panorama identified below.

44. Upon information and belief, Goodzone TV is a for profit organization with a principal place of business located at 2508 Coney Island Avenue, 2<sup>nd</sup> Floor, Brooklyn, NY 11223. Goodzone TV owns and operates the website [www.gudzon.tv](http://www.gudzon.tv), which provides unauthorized access to video streams of pirated versions of the Programming to paying subscribers in the United States.

45. According to WHOIS.com, a search engine that reveals the registrars of different websites, the registrar of that website is GoDaddy.com, LLC which is located at 14455 N. Hayden Rd., Ste. 226 Scottsdale, AZ. 85260. Annexed hereto as **Exhibit 7** is a screenshot of the WHOIS website showing that GoDaddy.com hosts the website [www.gudzon.tv](http://www.gudzon.tv).

46. Upon information and belief, Defendant Moidom engages in infringing activity using the IP address 50.62.23.145 by offering pirated versions of the Programming that had been intercepted from satellite communications to paying subscribers in the United States.

47. According to MOIDOM's website, its main office is located at 6005 Vineland Ave, Unit 103, North Hollywood, CA 91606.

48. Upon information and belief, MOIDOM is operated by Moidom LLC, a New York Limited Liability Company, which, according to New York Department of State Records is located at 140-25 Mulberry Avenue, Flushing New York with Dmitriy Yaroslavskiy listed as the agent for service of process. Annexed hereto as **Exhibit 8** is the entity information concerning Moidom LLC maintained by the New York Department of State.

49. The true name of Defendant TELEPROM which provides unauthorized access to video streams of pirated version of the Programming is unknown to Plaintiffs at this time. TELEPROM is the owner and operator of the domain [www.teleprom.tv](http://www.teleprom.tv).

50. TELEPROM operates a helpline at the 718 area code, thus subjecting it to jurisdiction in the State of New York.

51. Not only is TELEPROM believed to offer the Programming directly to consumers, but also, on information and belief, is a "wholesale" intermediate piracy source of streaming content consisting of intercepted satellite communications comprising the Programming for, *inter alia*, other Streaming Defendants in this action.

52. As the true name or owner of defendant VDALI which provides unauthorized access to video streams of a pirated version of the Programming to paying subscribers in the United States is unknown to Broadcasters, Broadcasters have sued defendant John Does. Defendant VDALI is known to Broadcasters only by the infringing website at the URL <https://vdali.tv>.

53. Together, Panorama, Asaf, Zeltser, Goodzone, Moidom, Teleprom, Vdali, and MHCOM shall be referred to herein as “Streaming Defendants.”

54. Upon information and belief, Defendant Vdali engages in infringing activity using the IP addresses 104.20.190.26 and 104.20.191.26 by offering pirated versions of the Programming that had been intercepted from satellite communications to paying subscribers in the United States.

55. Upon information and belief, defendant MHCOM GmbH is a vendor with a principal place of business at Kürbacher Weg 1, 86154 Augsburg, Germany which intercepts, transmits, sells or otherwise provides Broadcasters’ illegally intercepted programming to certain Streaming Defendants. Attached hereto as **Exhibit 9** is an invoice showing this transfer to an infringer.

56. Defendant John Does 1-50 are persons whose identities are unknown, but who are directing and contributing to the statutory violations and infringements herein.

### **JURISDICTION AND VENUE**

57. The Court has exclusive subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338 with respect to Broadcasters’ federal statutory claims and may assert supplemental jurisdiction over all other claims pursuant to 28 U.S.C. § 1367.

58. The Court also has diversity jurisdiction pursuant to 28 U.S.C. § 1332 because this controversy is between citizens of a foreign state and citizens of a state and the amount in controversy exceeds \$75,000.

59. Defendants are subject to personal jurisdiction in the Southern District of New York because they are located in (or within 100 miles of) this judicial district, conduct business

in this judicial district, and have engaged in tortious conduct outside the jurisdiction causing damage within the jurisdiction making long arm jurisdiction appropriate under New York law.

60. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 (b) and (c) and 1400 (a).

**ALLEGATIONS COMMON TO ALL DEFENDANTS**

61. This is an action to restrain the unauthorized interception of foreign satellite “over the air” transmissions and to restrain subsequent re-broadcasts, transfers and re-transmissions of valuable foreign language television programming through unauthorized video streaming over the internet to paying subscribers in the United States in violation of federal and state law and for damages.

62. Broadcasters produce and distribute Russian-language television programming and licensed content (“the Programming”) that is first broadcast in the Commonwealth of Independent States (“CIS”), including Russia and associate states Ukraine and Turkmenistan, and Estonia, Lithuania, Latvia and Georgia via satellite (the “Footprint”).

63. A satellite “footprint” is the geographic area over which a communications satellite’s transponders offer coverage.

64. Broadcasters distribute the Programming, in the first instance, via transmission to a satellite. Annexed hereto as **Exhibit 10** is a chart showing the satellites used by the various Broadcasters (“the Satellites”).

65. Accordingly, the “Programming” consists entirely of “radio-originated communications” within the meaning of 47 U.S.C. §605(a).

66. The Programming that Broadcasters transmit to the Satellites is encrypted in a manner to ensure that only authorized recipients may lawfully access it.

67. The Satellites then transmit the Programming to the Footprint.

68. Only certain persons within the Footprint are authorized by Broadcasters to receive the satellite transmissions.

69. Authorized recipients may include individuals living within the Footprint with satellite dishes who may view the Programming for personal use in exchange for a subscription fee.

70. Authorized recipients may also include cable operators operating within the Footprint who are authorized to receive satellite transmissions and then redistribute the Programming via an approved cable system to consumers within a limited geographic area within the Footprint.

71. To permit authorized recipients to view the Programming, Broadcasters ordinarily issue de-encryption devices that permit the satellite transmission to be viewed.

72. These de-encryption devices effectively control distribution of the Programming and permit access by authorized recipients only.

73. Broadcasters own and operate numerous famous television channels (each a “Channel” and collectively the “Channels”) that collectively form the Programming.

74. Each Channel bears a prominent trademark or trademarks and consist principally of copyrighted programs owned by each respective Broadcaster and protected under Russian copyright law, and contains repeated identifications of the Programming’s source.

75. The Programming in its totality as a compilation of copyrighted works is protected by Russian “neighboring rights” under the Civil Code of the Russian Federation Article 1332 irrespective of whether or not a Broadcaster owns the underlying copyrighted works forming the Programming.

76. “Neighboring rights” refers to a Broadcaster’s right under Russian law to the totality of the content, including the selection and arrangement of the Programming, regardless

of whether certain copyrightable elements have been licensed from a third party, such as a Hollywood film that a Broadcaster may have licensed for the Footprint only.

77. Each Defendant is engaged in the unauthorized interception, copying, retransmission, and distribution of encrypted transmissions of these Broadcasters' famous Channels and Programming through video streaming to paying consumers in this judicial district and throughout the United States in violation of, among other things, Section 605 of the Federal Communication Act 42 U.S.C. §605; the Lanham (Trademark) Act 15 U.S.C. §1501 et seq., Copyright Act 17 U.S.C. §101 et seq., and Section 349 of the New York General Business Law, each of which provides for injunctive relief and damages, together with costs and reasonable attorneys fees to a prevailing party.

78. Without discovery, Broadcasters are unable to plead additional facts as to how satellite transmissions are being intercepted, transferred and streamed by each particular defendant. Upon information and belief, certain Defendants may rely on third parties to intercept satellite communications on their behalf. Accordingly, such third parties are sued herein as John Does 1-50.

#### **ALLEGATIONS RELATED TO STREAMING ACTIVITIES**

79. Streaming Defendants offer streaming services on a similar business model. Each sells, without authority of the Broadcaster who owns the Programming, from their own domain name, the Programming as a streaming service to subscribers in the United States and particularly in this judicial district.

80. Defendant Teleprom is, on information and belief, engaged in the piracy of the Programming from satellite transmissions by intercepting satellite communications, de-encrypting them and re-transmitting them to one or more Defendants.

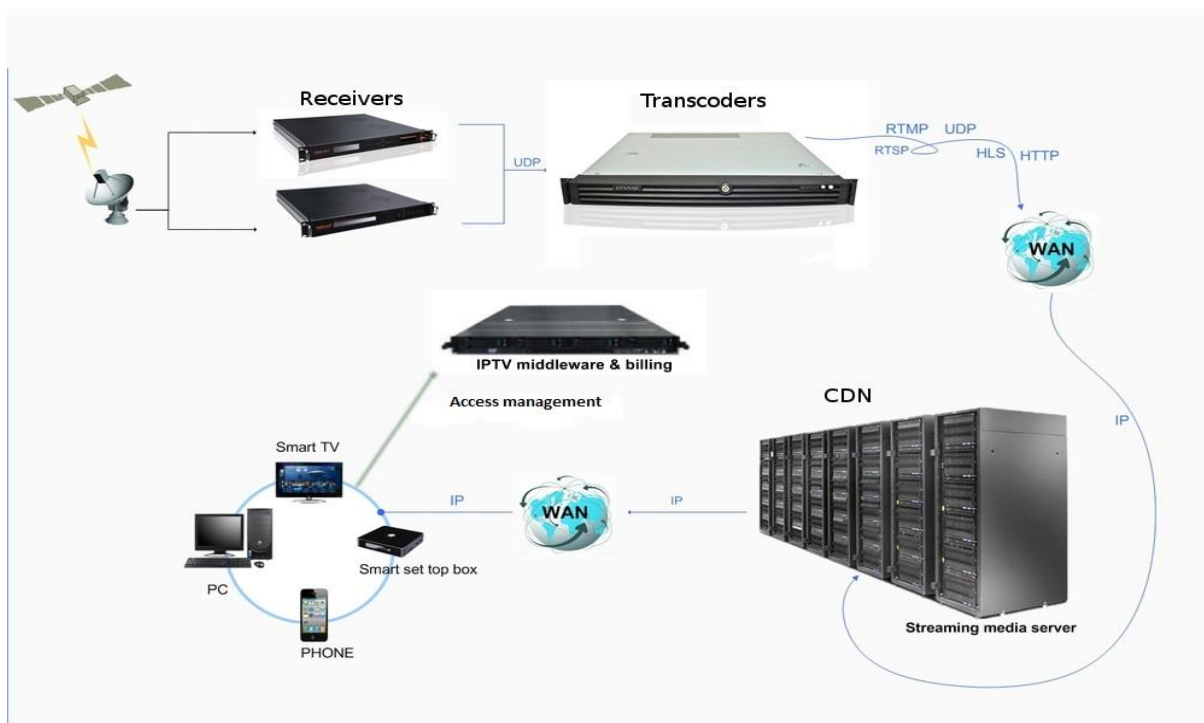
81. On information and belief, Teleprom supplies certain defendants with a feed of the Broadcasters' signals that have been decrypted.

82. Defendant MHCOM is, on information and belief, engaged in the piracy of the Programming from satellite transmissions by intercepting satellite communications, decrypting them and re-transmitting them to one or more Defendants.

83. On information and belief, MHCOM supplies certain defendants with a transcoded feed of the Broadcasters' signals that have been decrypted.

84. Defendants Asaf Yevdayev and David Zeltser, the "Individual Defendants", are officer or directors of Panorama or are otherwise personally engaged in the conduct attributed herein to Panorama.

85. For purposes of clarity, all unauthorized streaming of the Programming alleged herein, upon information and belief, consists of data from intercepted "over the air" satellite communications belonging exclusively to Broadcasters, upon information and belief, through a process substantially as illustrated below



86. In the illustration above, each Streaming Defendant provides “access management” and billing to U.S. consumers using an IPTV middleware and billing software suite.

87. The IPTV middleware and billing software suite is located on a relatively small server operated by each Streaming Defendant.

88. Using the “smart set top box” illustrated above, consumers who pay monthly fees to a Streaming Defendant launch a password-protected browser to that first contacts Streaming Defendant’s middleware, which, in turn issues an authorization permitting a consumer to access a streaming media server.

89. The streaming media server, in turn, delivers video content, in this case, the Programming.

90. Streaming media servers are hosted and run by large content delivery networks (“CDNs”).

91. As shown in the illustration above, it is believed that each Broadcaster distributes its encrypted content via satellite, which, upon information and belief is de-encrypted by a receiver, recorded and transcoded, and then sent to a CDN.

92. It is believed that either the Streaming Defendant (or the Defendant’s agent sued herein as John Doe) uses a form of de-encryption to access satellite broadcasts of the Programming in the geographic footprint of the respective satellite (for example, the Ukraine) as a first step in delivering the illegal streaming services.

93. As a second step, upon information and belief, Defendants or their agents use sophisticated digital recorders to transform the satellite signals into digital data to be transmitted via the Internet.

94. As a third step, upon information and belief, Defendants provide unauthorized streaming services of the Programming to an internet protocol address via a third party internet service provider.

95. As a fourth step, upon information and belief, the Streaming Defendants sell passwords and monthly subscriptions that permit individual consumers to access internet protocol addresses from which the consumers can view the Programming without permission from the Broadcasters in this judicial district.

96. The Streaming Defendants' infringement is accomplished and facilitated in part by sales to consumers in the United States through the use of interactive websites at which consumers located in this judicial district purchase and receive access to the Programming; [www.mypanorama.tv](http://www.mypanorama.tv); [www.gudzon.tv](http://www.gudzon.tv), <https://moidom.tv/>, <https://vdali.tv>, and <http://teleprom.tv> ("the Websites") registered, hosted and operated in the United States.

97. The IPTV player software provided by each Streaming Defendant permits consumers to watch the Channels and Programming on various consumer electronics including televisions, computers and hand-held devices.

98. A consumer using the IPTV software (browser) on set-top boxes or downloaded from the Websites can, by using a password provided by a Streaming Defendant, access a unique Internet Protocol ("IP") address from which the consumer can access a stream of the Programming provided by the Defendants through a CDN.

99. In the alternative, Streaming Defendants' unauthorized streaming may derive from data stolen from a cable system in violation of 47 U.S.C. §553, but in the absence of discovery, Broadcasters are unable to verify this and currently believe that the most likely source of pirated Programming is satellite transmissions as illustrated above.

100. The Streaming Defendants market access to the Programming to U.S. consumers within this judicial district for a monthly fee.

101. The Streaming Defendants mislead consumers by making it appear on their Websites that they have the right to rebroadcast Broadcasters Programing and Channels by, among other things, displaying the Channels' respective trademarks.

102. The Streaming Defendants accept electronic or telephone payments. Bank transfer, MasterCard, VISA, Discover, American Express and PayPal are among the most commonly accepted payment methods.

103. When a U.S. consumer makes a payment to a Streaming Defendant, the consumer is typically invited to download an internet protocol television ("IPTV") player or purchase a set-top box that permits end-user consumers to bypass the Broadcasters' encryption to view the Programming.

104. Upon information and belief, the Streaming Defendants use affiliates or similar corporations, sued as John Does herein, with different names to process payments received from U.S.

105. Upon information and belief, IP addresses and the streaming services are administered and maintained by Defendants together with John Does who are contributing to the infringements described herein.

106. The Streaming Defendants' unlawful streaming services have been offered at far lower prices than lawfully licensed services to thousands of subscribers. This has caused Broadcasters a loss of subscriber revenue, market share, and advertising revenues. Each Streaming Defendant who operates a streaming service inflicts irreparable harm on the Broadcasters every day that the streaming service remains in operation.

107. The Streaming Defendants are parasitic on the legitimate outlets for their Russian-language broadcasts. Having subscribed to the illicit broadcasts, such customers would be unlikely to simultaneously subscribe to the legitimate ones. Once a certain month has passed, there is no way to restore demand for a legitimate subscription for that month. For that reason, the Streaming Defendants inflict irreparable harm on Broadcasters.

108. The Streaming Defendants have arranged their affairs as to limit their exposure to a possible money judgment. As discovery to date has shown, at least some Defendants do not keep proper records, have sought to evade jurisdiction or engaged in other conduct that indicate that either a money judgment or mild forms of injunctive relief (e.g., prohibiting Defendants from illegally distributing the Broadcasters Programming) may not be effective in granting the Broadcasters effective relief.

109. Moreover, the customers obtain their illicit access to the Programming through the Websites and their domain names. To the extent that any Streaming Defendant has “blue sky” in its domain name, that asset has been acquired through an illegal business – selling unauthorized access to the Programming and that asset is therefore an illicitly gained one.

110. For that reason, the Broadcasters request that the Court order the Streaming Defendants, or if necessary their domain registrar, to disable their domain names hosting the Websites and place the domain names under a registry hold rendering them nontransferable pending the outcome of this litigation.

111. Broadcasters request that the Court order such domain names be transferred to the Broadcasters. Such an outcome is fair and equitable because these domains are dedicated entirely to infringing the Programming and thus have no legitimate “blue sky” from which the Streaming Defendants should be permitted to profit.

112. Unless restrained by this Court, the Streaming Defendants' actions will continue to cause irreparable harm resulting from Broadcasters' loss of control over the distribution of Broadcasters' Channels and Programming, the preemption of Broadcasters' opportunities to license content over new media, and the continued unlawful conduct contemplated by Streaming Defendants threatens Broadcasters with substantial irreparable losses.

#### **ALLEGATIONS SPECIFIC TO INFOMIR DEFENDANTS**

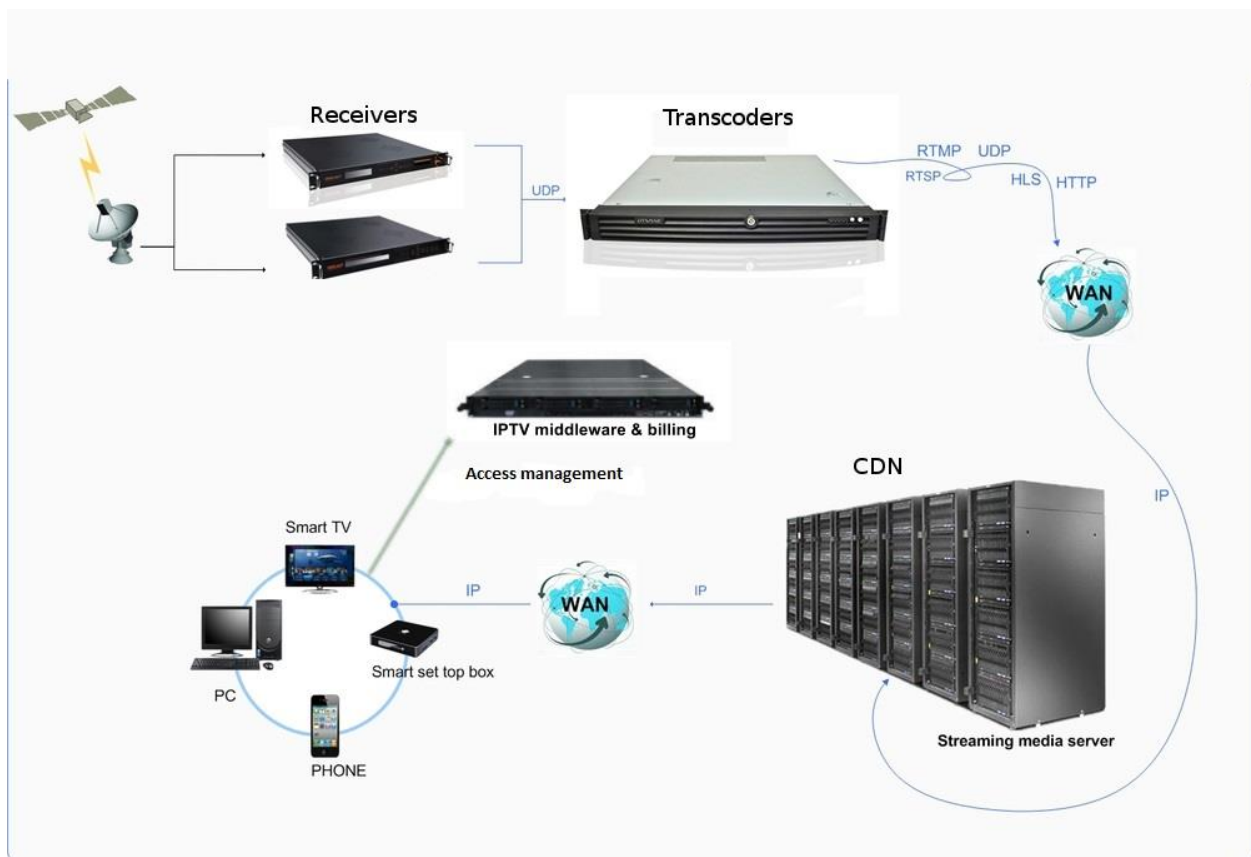
113. Infomir and Infomir GmbH also offer unauthorized access to the Programming through software that is configured to operate set-top boxes that are pre-configured to assist piracy and that are manufactured by Teletec.

114. Such set-top boxes are either preloaded with apps that are designed to give unauthorized access to the Broadcasters Programming, or purchasers of these boxes are directed to a website to download software developed by Infomir capable of doing so.

115. Upon information and belief, Infomir Defendants provide unauthorized streaming services of the Programming to subscribers in the same way that the Streaming Defendants do.

116. Upon information and belief, the Infomir Defendants manufacture and sell set-top boxes without pre-loaded software under the MAG brand name. Using the MAG set-top boxes, Infomir Defendants then encourage piracy in two ways: (a) the Infomir Defendants market the MAG set-top boxes to other John Doe pirates and encourage such John Does to set up piracy operations; and; (b) the Infomir Defendants encourage consumers who have purchased the MAG set-top boxes to then pay additional fees to purchase monthly or yearly subscriptions to unauthorized streams from the Streaming Defendants that can then be viewed through the boxes manufactured and sold by the Infomir defendants.

117. In the illustration below, the Infomir Defendants sell to consumers and to Streaming Defendants the “smart set top box” that is pre-loaded with an operating system and browser that permits consumers to gain access to the Programming. Additionally, the Infomir Defendants provide the “access management” and configuration of the IPTV middleware and billing by making downloads available to Streaming Defendants and John Doe pirates. As illustrated below, using the MAG or AURA set-top boxes, consumers who subscribe to the Streaming Defendants and John Doe defendants’ streaming services can watch the Programming on their devices such as smart TVs, personal computers and mobile phones:



118. Infomir GmbH is either acting in its own right or in active concert and participation with Infomir, other Defendants and John Does to supply the Programming both to consumers directly, and indirectly to multiple distributors that it teaches to use Stalker software and supplies with MAG set-top boxes.

119. The Infomir Defendants also sell set-top boxes under the AURA brand name that are pre-loaded with apps that connect directly to unauthorized versions of the Programming supplied by the Infomir Defendants that have been intercepted and retransmitted from decrypted satellite communications.

120. The MAG and AURA set-top boxes are configured primarily to facilitate piracy in several ways.

121. First, the MAG and AURA set-top boxes access domains that do not have extended validation certificates (indicated by an “https” prefix) that facilitate copyright protection, blacklisting and monitoring that are industry standards.

122. The extended validation certificates provide additional security in that the domain certificates contain information about the owner of the domain. The additional measures confirm the identity of the owner and also guard against third-party eavesdropping.

123. Infomir LLC and Infomir GMBH operate the websites [www.infomir.us](http://www.infomir.us), [infomir.eu](http://infomir.eu) and [www.infomirusa.com](http://www.infomirusa.com) from which MAG and AURA boxes can be purchased.

124. The Federal Communications Act at 47 USC §605(e)(4) imposes liability on “[a]ny person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a)”.

125. The Infomir Defendants are, on information and belief, in violation of Section 605(e)(4) by their manufacture importing and distribution of set-top boxes. The set-top boxes are a “device or equipment” that the Infomir Defendants know or should know is “primarily of assistance in the authorized decryption of satellite cable programming” because the Infomir

Defendants design and distribute Stalker Middleware that is designed to retransmit unauthorized content behind a paywall to assist infringers.

126. Infomir sells set-top boxes with the primary purpose of the unauthorized decryption of satellite programming and other forbidden activities listed in 47 USC §605(e)(4). The set-top boxes operate in conjunction with software – either pre-loaded in the case of the Aura boxes or with an Infomir-designed software program known as “Stalker Middleware.” The purpose of the software is to manage the distribution of the video streams to MAG and AURA set-top boxes.

127. Infomir’s Stalker Middleware software is a key component, distributed by Infomir, that transforms the MAG box into a vehicle for large-scale infringement. The Stalker Middleware software is, on information and belief, developed, owned, and controlled by Infomir.

128. The purpose of the Stalker Middleware software is to allow a user to set up networks over which the user can distribute IPTV to its own customers. These networks allow decentralized but massive infringement of the Broadcasters’ rights.

129. According to one technology wiki specializing in media technology, “Stalker Middleware is an Infomir company software designed to organize IPTV and OTT projects which allows for a fast and efficient launch of IP-network video services. The key feature of Stalker Middleware is the ability to run a service based on IP networks with minimum initial investment and very short time.’ See [http://kodi.wiki/view/PVR/Backend/Stalker\\_Middleware](http://kodi.wiki/view/PVR/Backend/Stalker_Middleware).

130. On July 19, 2012, the website IBXT.com conducted an interview with the director of Infomir, Alexander Marahovsky <http://www.ixbt.com/editorial/interview-infomir-2012.shtml> (**Exhibit 11** together with a certified English translation) Of note, Marahovsky states that:

A competitive advantage that beneficially distinguishes us from all other manufacturers, is the correct priority system: we guarantee the quality and reliability of the device, we carry out constant modernization and expansion of

functionality, as well as provide local technical support to the users. And most importantly, we offer the best market price for IPTV solutions. We place the main emphasis in our strategy for entering this market on a connection to the country and the language of the user, which is unique among analogous decisions. In contrast to foreign media players, we do sell not the consumer a ‘bare device’ but those services that are demanded by the specific language group: more than 100 channels of Internet tv (mostly in Russian), over 200 Internet radio channels, access to more than 10 leading online cinemas within the CIS. There is an abundant selection of media players on the market but those who can provide our customers access to high-quality Russian-speaking tv/video content -- those are few and far between.

**Exhibit 11** at 3

131. Infomir has failed to undertake any anti-piracy upgrade, despite Marahovsky’s admission that Infomir is capable of controlling the functionality of the set-top box and Stalker Middleware.

132. Additionally, Infomir’s director admits that Infomir does not sell the consumer a “bare device,” but that it instead provides consumers with access to streams of “high-quality Russian-speaking tv/video content.”

133. Indeed, Infomir’s boxes are sold from vendors such as Amazon with pre-loaded IPTV subscriptions to potential infringing websites. Attached hereto as **Exhibit 12** is a screenshot of an Amazon page offering a MAG 254 IPTV Box with a preloaded subscription.

134. Infomir’s own marketing materials show that the boxes are sold with the knowledge and with the intent to promote uses in violation of 47 USC §605(e)(4). Infomir’s own website begins its discussion of the set-top boxes by stating: “Interested in starting an interactive television business?” Annexed hereto as **Exhibit 13** is a true copy of Infomir’s website displaying this information.

135. Furthermore, there are widely posted videos at YouTube and other video sharing sites with titles promoting piracy such as: “HOW TO SET UP A MAG 254 SET TOP BOX &

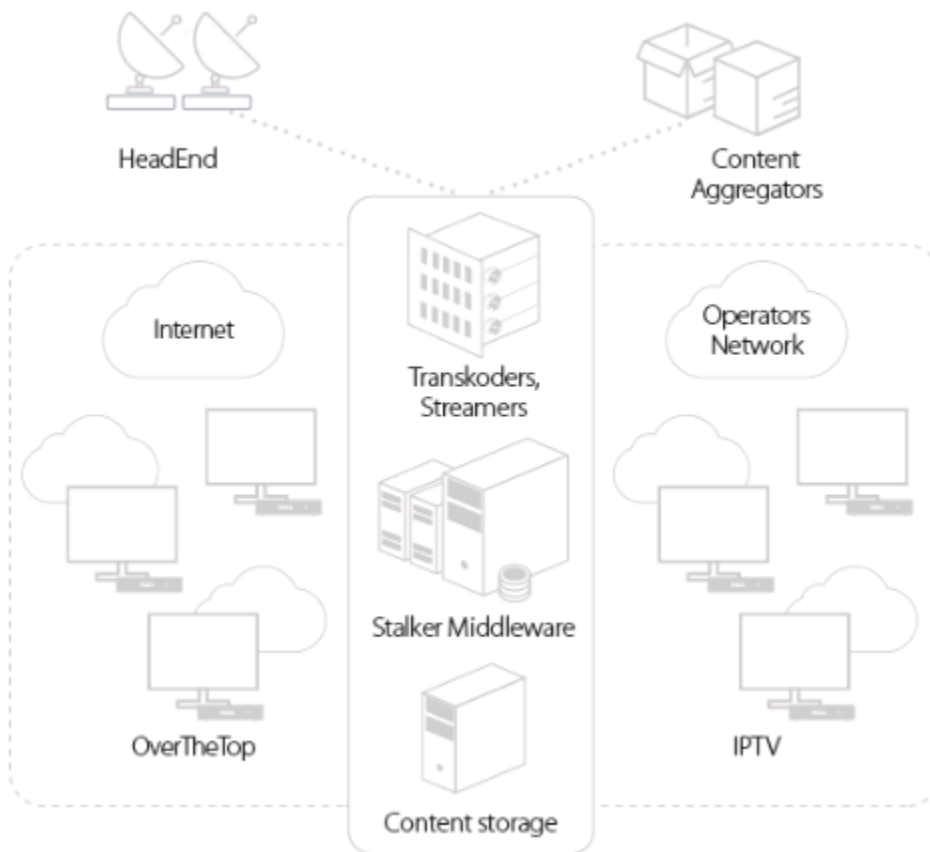
BECOME A CABLE COMPANY”. (See <https://www.youtube.com/watch?v=dgslslUCmLI>)

Infomir knows or should know about the proliferation of such videos.

136. As described on its website, Infomir also attends certain trade shows to market its boxes to would-be infringing middlemen pirates encouraging them to set up networks of infringing subscribers using the Infomir boxes. Infomir encourages its customers to become distributors of infringing television broadcasts by showing them how they can resell Infomir boxes to their customers, then charge those customers for access to an illicit feed.

137. Infomir profits from the infringement of broadcasts that are otherwise restricted to paying subscribers, and upon information and belief, Infomir controls one or more offshore pirate entities providing infringing content.

138. In fact, Infomir offers something called the “MAGic Solution” in connection with its MAG boxes. The website at the domain [www.infomir.eu](http://www.infomir.eu) shows a diagram of a proposed set up of an IPTV (or OTT) network for a would-be pirate to use in infringing others’ rights as illustrated in the diagram below:



139. The MAGic Solution shows that Infomir’s boxes and Stalker Middleware are designed to promote for the set-up of groups of subscribers.

140. Referring to the diagram in **Exhibit 13**, the “content aggregators” are legitimate channels such as the Broadcasters here.

141. Although Infomir tries to cloak the purposes of these boxes in innocuous language such as “project”, Infomir makes clear that the end use of these boxes is to promote piracy. The language suggesting that an Infomir customer can become an “interactive television business” reveals the commercial purposes behind these boxes.

142. In laying out the MAGic Solution, Infomir shows the components necessary to begin an infringing business, a box (provided by Infomir), Stalker middleware, which is free, a

server, which can be purchased or rented, and the final component, content, that Infomir suggests can be “provided by operator himself” and is followed by the following disclaimer: “Please notice that Infomir company is not a content provider, and does not provide software and equipment for access to any kind of content. Infomir company offers technical solution only that allow to offer IPTV/OTT services. Any content issues should be solved with rights owners of the content you need in your region.”

143. Upon information and belief, the vast majority of Infomir’s customers, if not all, are infringers.

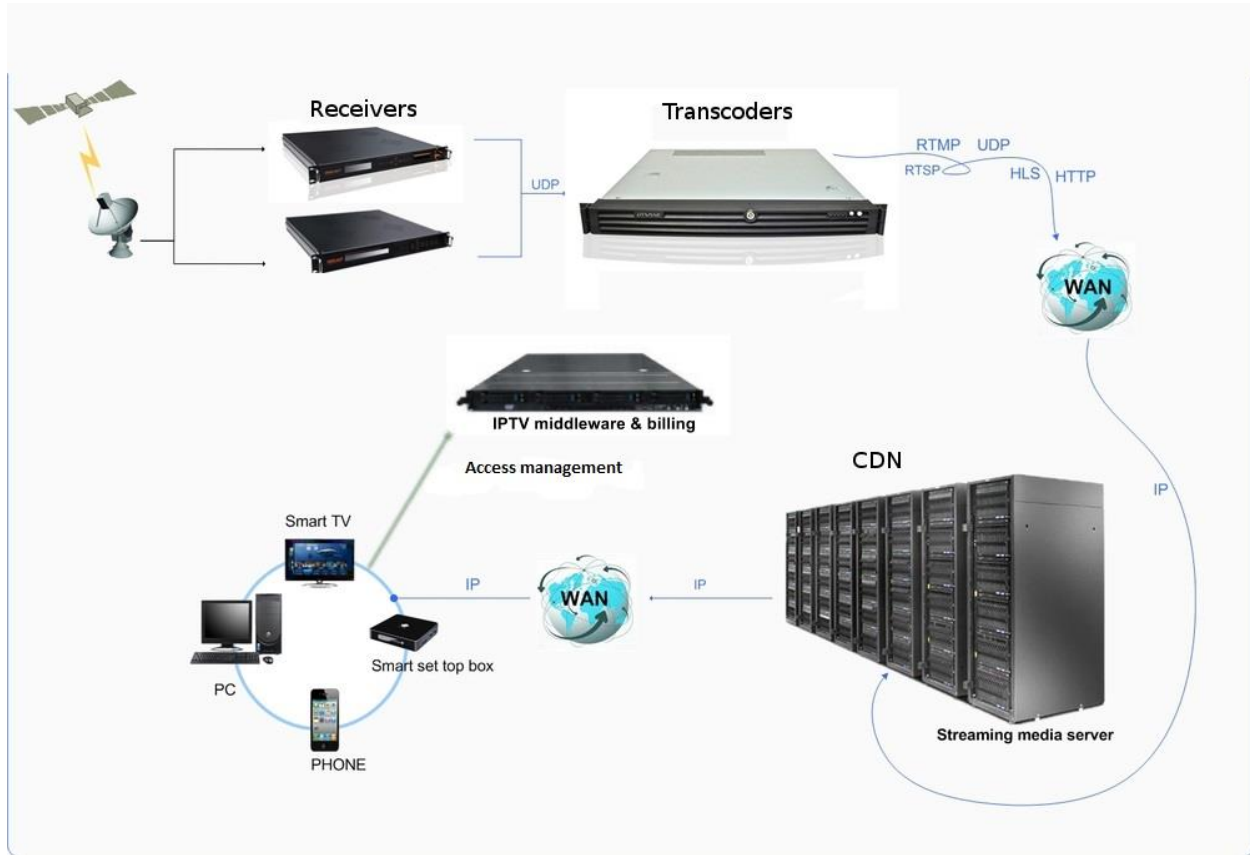
144. Presentations such as these show that Infomir is inviting its customers to engage in infringing uses of its technology. Furthermore, Infomir cannot show that its products – either hardware or software—are actually being used in a non-infringing fashion. A theoretical non-infringing use is not enough to insulate Infomir from liability.

145. Even though Infomir attempts to cloak its purposes behind this purported warning, the fact that these boxes are used to pirate from legitimate sources is clear. The diagram of the system in **Exhibit 13** clearly shows satellite receivers and a head-end, which is technology used by commercial broadcasters such as the Broadcasters here.

146. The business model suggested by Infomir clearly indicates that the purpose of it is to provide access to the “content”. The only reasonable expectation is that content that customers will pay for is that which is only otherwise available for a fee, such as the Programming.

147. The Infomir MAGic Solution is merely a just-add-water recipe for infringement on a massive scale— where the water is access to an illicit feed of the Broadcasters’ Channels. Such feeds may be provided by third-parties or others acting in concert with Infomir.

148. The process by which Infomir's set top boxes are able to access the Programming is detailed in the chart below, where the Aura or MAG boxes are the "Smart set top box" and Stalker is the "IPTV middleware & billing."



149. Additionally, Infomir retains the technological ability to filter out and block pirates on its set-top boxes and the practical ability to disable the use of the software of others, but fails to do so. When users log into Infomir's set-top boxes, the box itself has browser or browser-like software that enables it to connect to internet addresses. At log-in, the Infomir box checks with a particular address where the latest version of the Infomir firmware is stored. The firmware is updated periodically.

150. That web address instantly checks the user's set-top box to see if the firmware is up-to-date. If that firmware is not up-to-date, the Infomir box downloads the latest version of the firmware program.

151. Thus, Infomir's claims to be purely a hardware company are false. Not only because of its development of the Stalker Middleware software and the programs used in the AURA boxes, but also because Infomir maintains a measure of control over the user's box that is used to periodically update the firmware residing on it.

152. Infomir's periodic updates to set-top boxes could be used to provide an industry-standard level of antipiracy measures, such as pre-approving apps (using closed devices) and blacklisting.

153. Blacklisting involves the blocking of access to websites which do not maintain extended validation certificates that, when implemented properly, would indicate that the websites are secure locations in which to enter payment information, logins and passwords.

154. Blacklisting would involve the blocking of access to websites like mypanorama.tv and teleprom.tv which are not secure websites that maintain extended validation certificates.

155. The Infomir Defendants have failed to issue software updates to their MAG and AURA set-top boxes that would prevent consumers from accessing the streams of known infringers.

156. An additional anti-piracy measure that could be undertaken by the Infomir Defendants is manufacturing closed devices. Closed devices can only download pre-approved apps and connect to pre-approved streams from Infomir's closed market. This is similar to how an Apple iPhone can only download pre-approved apps from the Apple Store in order to ensure that Apple devices are not used for piracy.

157. The Infomir Defendants' manufacturing and selling boxes to consumers without adequate anti-piracy measures ensure that the MAG and AURA boxes will be primarily used for infringing activity.

158. As Marahovsky admits in his interview, Infomir is doing business in the United States stating that "in Germany and in America there is a distribution and in Germany there is a local production for the EU market" (**Exhibit 11** at 4)

159. As Marahovsky admits, "in each country, [Infomir has] a partner who, in particular, provides service and support. These are the same companies that are engaged in retail within the territory of a respective region." (**Exhibit 11** at 4). Upon information and belief, Marahovsky refers to Infomir LLC as the U.S. "partner."

**THE CHANNELS AND PROGRAMMING ARE SUBJECT TO PROTECTION  
PURSUANT TO THE COMMUNICATIONS ACT**

160. Broadcasters are "aggrieved parties" within the meaning of Section 605(d) of the Federal Communication Act because each Website and Infomir Defendant's unauthorized streaming violates Broadcasters' proprietary rights in the initial transmissions of the Channels and Programming, as well as violating Broadcasters' proprietary rights in Broadcasters' capacities as wholesale and retail distributors of the transmissions. 42 U.S.C. § 605 (d)

161. Section 605(a) of the Federal Communication Act forbids unauthorized rebroadcasts in the United States of foreign satellite transmissions. 42 U.S.C. § 605 (d)

162. Section 605(a) of the Communications Act expressly provides that the Act's protections extend to any "foreign communication" that is sent from or received in the United States.

163. The Programming and Channels are both broadcast into the United States from the Russian Federation in the first instance.

164. Therefore, the Programming and Channels are “foreign communications” subject to protection under the Communications Act.

165. Broadcasters’ broadcasts are initially transmitted as “radio communications” within the meaning of the FCA in that they originate as satellite transmissions. See **Exhibit 10**, a representative summary of each of the broadcasters’ channels and the satellites through which their broadcasts are transmitted.

166. Such satellite transmissions are intended for receipt by local distributors’ “head-ends”, which are then distributed to authorized recipients by the local distributor.

167. The Streaming Defendants and Infomir Defendants intercept these broadcasts downstream of the satellite transmission. In the alternative, the Streaming Defendants and Infomir Defendants receive the Broadcasts knowing that such Broadcasts have been illegally intercepted downstream of a satellite transmission.

168. On information and belief, the Streaming Defendants and Infomir Defendants obtain access to the decrypted signals either directly or by agreement with other parties located abroad.

169. On information and belief, Streaming Defendants decrypt broadcasts by either “user cards” or “operator cards” which are hardware designed to decrypt the Broadcasters’ signals. User cards allow for the decryption of one channel and are designed to be used by the retail subscribers in Russia or Russia’s near-abroad. Operator cards are intended for use by local cable operators and allow for the decryption of multiple channels.

170. On information and belief, by deploying multiple user or operator cards, Streaming Defendants make a broad range of Broadcasters’ channels (including local variations by city, etc.) available.

171. On information and belief, Streaming Defendants and their agents feed off illicitly decrypted broadcasts available to local resellers. On information and belief, defendant TELEPROM is engaged in such activity.

172. All Defendants provide access to the Programming through the use of domains that their subscribers connect to. By providing a login and password given to them by a Streaming Defendant using Stalker Middleware, these subscribers can view the Programming illicitly and receive bills generated by Stalker Middleware.

173. Infomir provides access to the Programming through MAG and AURA set-top boxes which it sells. Such set-top boxes are either pre-loaded with software specifically designed to access the Broadcasters' channels or by directing customers to a website where a so-called "middleware" program known as Stalker Middleware can be downloaded and used by pirates to access and exploit the Broadcasters' channels.

174. Infomir's set-top boxes then access an internet domain or domains through which a U.S. subscriber can then view the Broadcasters' channels.

**THE CHANNELS AND PROGRAMMING ARE SUBJECT TO  
PROTECTION PURSUANT TO THE BERNE AND PARIS CONVENTIONS**

**A. Broadcasters Have Standing Under The Copyright Act Pursuant To The Berne Convention**

175. Both the United States and the Russian Federation are signatories to the Berne Convention for the Protection of Literary and Artistic Works ("Berne Convention").<sup>2</sup>

176. Pursuant to the terms of the Berne Convention and the implementing statutes in the signatory countries thereto, each signatory country is obligated to afford the same protection

---

<sup>2</sup> The Berne Convention came into force in the United States on March 1, 1989 and in the Russian Federation on March 13, 1995. See [http://www.wipo.int/treaties/en/ShowResults.jsp?treaty\\_id=15](http://www.wipo.int/treaties/en/ShowResults.jsp?treaty_id=15) (last accessed November 4 2015).

under its copyright laws to a work originating in another of the signatory countries as it would to a work originating within that country. Thus, each signatory country of the Berne Convention is obligated to recognize and enforce Broadcasters' copyrights in the Channels and Programming as they would if the Channels and Programming had originated in that country. The United States Supreme Court has consistently upheld the Berne Convention and indicated the strong public policy behind the United States accession into it. *Golan v. Holder*, 33 ITRD 1769, 132 S. Ct. 873, 878, 181 L. Ed. 2d 835 (2012).<sup>3</sup>

177. The Programming constitutes Berne Convention works as defined in the Copyright Act, Title 17 U.S.C., § 101, as amended, and is subject to the protection of the Copyright Act of 1976, Title 17 U.S.C. §§ 101 et seq. This is because the Berne Convention extends to cinematic works. (Art. 2(1)).

178. Subject to limited exceptions, the Programming relevant hereto is produced and broadcast in the first instance Russian Federation, and therefore registration of the Programming with the United States Copyright Office is not required for Broadcasters to assert claims in this Court. *See Itar-Tass Russian News Agency v. Russian Kurier, Inc.*, 153 F.3d 82, 90 (2d Cir. 1998); *Kuklachev v. Gelfman*, 600 F. Supp. 2d 437, 474 (E.D.N.Y. 2009).

179. Additionally, Broadcasters' Channels and Programming are protected by the intellectual property laws of the Russian Federation and are therefore entitled to the protection of United States copyright and trademark laws pursuant to international conventions, including

---

<sup>3</sup> "Members of the Berne Union agree to treat authors from other member countries as well as they treat their own. Berne Convention, Sept. 9, 1886, as revised at Stockholm on July 14, 1967, Art. 1, 5(1), 828 U.N.T.S. 221, 225, 231–233. Nationals of a member country, as well as any author who publishes in one of Berne's 164 member states, thus enjoy copyright protection in nations across the globe. Art. 2(6), 3. Each country, moreover, must afford at least the minimum level of protection specified by Berne. The copyright term must span the author's lifetime, plus at least 50 additional years, whether or not the author has complied with a member state's legal formalities. Art. 5(2), 7(1). And, as relevant here, a work must be protected abroad unless its copyright term has expired in either the country where protection is claimed or the country of origin. Art. 18(1)–(2)."

Russian “neighboring rights” in the Programming which protects the selection and arrangement of the programming, in addition to any underlying copyrighted works within the Programming.

180. Attached hereto as **Exhibit 14** is a true and correct translation of Articles 1329, 1330, 1331, and 1332 of the Civil Code of the Russian Federation (“Civil Code”).

181. Article 1332 of the Civil Code provides that all broadcasts that originate in the Russian Federation are protected by Russian law.

182. Russian law protects neighboring rights which, as relevant here, are the rights a broadcaster has in its broadcasts including the rights to re-broadcast its broadcasts. *See* Art. 1330.2 of the Civil Code which protects a broadcaster’s right to record; reproduce; distribute; and re-transmit its original broadcast.

183. Russian law does not require any formalities, such as registration, for a broadcaster to exercise neighboring rights.

184. Because the alleged infringement is occurring in the United States, domestic law applies to Broadcasters’ infringement claims. *Dish Network L.L.C. v. TV Net Solutions, LLC*, No. 6:12-CV-1629-ORL-41, 2014 WL 6685351, at \*3 (M.D. Fla. Nov. 25, 2014) *citing Itar-Tass*.

185. The Court may issue preliminary and permanent injunctive relief to stop illegal transmission of Berne Convention works over IPTV. *WPIX, Inc. v. ivi, Inc.*, 765 F. Supp. 2d 594 (S.D.N.Y. 2011) *aff’d*, 691 F.3d 275 (2d Cir. 2012) *lv. denied* 133 S. Ct. 1585, 185 L. Ed. 2d 607 (2013).

**B. Broadcasters Have Standing Under The Digital Millennium Copyright Act**

186. Section 1201 of the Copyright Act (as amended by the Digital Millennium Copyright Act (“DMCA”)) includes both anti-circumvention and anti-trafficking provisions

which prohibit the circumvention of any technological measure designed to control access to a work subject to the protection of the Act including the Programming. 17 U.S.C. § 1201

187. Defendants circumvent the copyright protections imposed by the Broadcasters on their broadcasts, or retransmit the Programming, knowing that another person obtained it through bypassing the Broadcasters' access controls.

188. Each Defendant is aware that the Broadcasters' signals are encrypted and have constructed a technological pathway around the legitimate protection measures imposed by each Broadcaster.

189. Upon information and belief, Defendants either knowingly and purposefully hack into or otherwise circumvent and intercept Broadcasters' encrypted satellite signals in violation of the DMCA or are in active concert and participation with those who do.

190. Defendants then download, copy or otherwise utilize the Broadcasters encrypted signals and rebroadcast and/or store them via equipment, including computer servers, located in the United States.

**C. Broadcasters Have Standing Under The Lanham Act Pursuant To The Paris Convention**

191. Both the United States and the Russian Federation are signatories to the Paris Convention for the Protection of Industrial Property.<sup>4</sup>

192. Broadcasters' Channels are identified by the marks reproduced under the "Parties" heading of this Complaint.

193. Section 44 of the Lanham Act provides foreign nationals the same rights and protections provided to United States citizens by the Lanham Act. Accordingly, Broadcasters may seek protection in this Court for violations of the Lanham Act. *Vanity Fair Mills, Inc. v. T.*

---

<sup>4</sup> The Paris Convention came into force in the United States on May 30, 1887 and in the Russian Federation on July 1, 1965. See [http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty\\_id=2](http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=2) (last accessed November 4, 2015).

*Eaton Co.*, 234 F.2d 633, 640 (2d Cir. 1956) *cert. denied* 352 U.S. 871 (1956) *rehearing denied* 352 U.S. 913 (1956).

### **FACTS EVIDENCING DEFENDANTS' UNLAWFUL CONDUCT**

194. Broadcasters are actively engaged in the production and distribution of the Programming and other copyrighted works primarily in the Russian language on their respective Channels. Broadcasters have entered into certain license agreements providing non-parties with the exclusive right to broadcast and re-broadcast their Programming and other copyrighted materials in the United States. Only the relevant license holders are authorized to broadcast, re-broadcast or otherwise transmit Broadcasters' protected, copyrighted programming and other materials in the United States via IPTV or otherwise.

195. Upon information and belief, IPTV was first developed in or about 1995 and has gained popularity as a broadcast medium.

196. Upon information and belief, Defendants hack, capture or otherwise acquire without permission the encrypted signals of the Broadcasters' Channels and transmit those signals to its servers which in turn stream the wrongfully acquired signals over IPTV to paying customers in this judicial district and elsewhere.

197. Annexed hereto as **Exhibit 15** is an investigator's affidavit dated June 24<sup>th</sup> 2016 containing screenshots detailing Defendant Infomir's unlawful conduct.

198. Annexed hereto as **Exhibit 16** is an investigator's affidavit dated August 18<sup>th</sup> 2016 containing screenshots detailing Defendant Goodzone's unlawful conduct.

199. Annexed hereto as **Exhibit 17** is an investigator's affidavit dated January 31, 2017 containing screenshots detailing Defendant Panorama's unlawful conduct.

200. Annexed hereto as **Exhibit 18** is an investigator's affidavit dated February 22, 2017 containing screenshots detailing Defendant Vdali's unlawful conduct as well as Teleprom's and Vdali's connection with Infomir.

201. Upon information and belief, to subscribe to Defendants' services, including unauthorized access to the Channels and Programming, an individual with internet access need only (a) access the Defendants' websites, (b) download software (e.g. the VLC Media Player) and/or receive equipment necessary for viewing the pirated content (see, e.g., **Exhibit 19**, Infomir's homepage offering receiver boxes), (c) subscribe to Defendants' service, (d) agree to the terms and conditions listed on the relevant website, and (e) pay the necessary charges and fees to Defendants.

202. Upon information and belief, Defendants have not obtained authorization from any Plaintiff to stream the Channels or Programming over IPTV or to broadcast or re-broadcast the Channels or Programming through any other method. Accordingly, in light of Defendants' conduct, consumers will likely be confused into believing that Defendants are authorized to broadcast or re-broadcast the Channels and the Programming.

203. While the Broadcasters allege that each of the Defendants is involved in wholesale copyright infringement, in order to provide a manageable complaint, the Broadcasters have identified the following representative programming in which each Broadcaster holds the copyrights and attach hereto true copies of programming schedules and examples of copyrighted programming for the broadcasters as **Exhibit 20**.

**CAUSES OF ACTION**

**COUNT ONE**

**UNAUTHORIZED PUBLICATION OR COMMUNICATION UNDER THE FEDERAL COMMUNICATIONS ACT**

**(AGAINST ALL DEFENDANTS)**

204. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

205. Broadcasters own the rights to, among other things, broadcast, re-broadcast, market and distribute within the United States and elsewhere their encrypted programs which are currently de-encrypted and distributed through the websites and software distributed by Defendants.

206. Broadcasters initially broadcast their programming through various satellites that are intended only for authorized recipients, who are local distributors.

207. Defendants intercept Broadcasters' broadcasts downstream of the satellite transmission.

208. Broadcasters license the rights to broadcast and re-broadcast their programs to certain third parties in exchange for a fee.

209. Defendants have not received a license from any Plaintiff to de-encrypt broadcast or re-broadcast its programs, nor has it received any other permission, express or otherwise, to do so. Through their Websites, Defendants have and continue to intentionally pirate, retransmit and publish Broadcasters' programs for the sole purpose of their own economic gain and to the detriment of Broadcasters and their licensees.

210. The foregoing willful and intentional actions of Defendants constitute the unauthorized publication or use of communications for commercial advantage in violation of 47

U.S.C. § 605(a), which is applicable to satellite and other cable communication pursuant to subparagraphs (b) – (e) of that section.

211. Without the express permission of any Broadcaster or Broadcasters collectively, Defendants are receiving, transmitting or assisting in transmitting interstate foreign broadcast communications by wire or radio, causing said communications, their contents and substance to be divulged and published through unauthorized channels of transmission or reception.

212. The foregoing willful and intentional actions by Defendants constitute the unauthorized publication or use of communications for commercial advantage in violation of 47 U.S.C. § 605(a).

213. “Any person aggrieved by a violation of subsection (a) may bring a civil action for actual or statutory damages for each violation.” 47 U.S.C. § 605(e)(3)(C). “Any person aggrieved” includes “any person with proprietary rights in the intercepted communication.” 47 U.S.C. § 605(b)(6).

214. As a direct and proximate result of Defendants’ wrongful actions, Broadcasters have sustained and will continue to sustain damages and irreparable harm such that monetary, preliminary and permanent injunctive relief is warranted as authorized by 47 U.S.C. § 605(e) along with an award of any such other relief the Court deems just, proper and equitable.

215. The Communications Act provides that the Court “shall direct the recovery of full costs, including awarding reasonable attorneys’ fees to an aggrieved party who prevails.” 47 USC § 605 (e)(3)(B)(iii). Accordingly, the Court should also award costs to Broadcasters, together with reasonable attorneys’ fees.

**COUNT TWO**

**SALES OF DEVICES PRIMARILY FOR THE USE OF OBTAINING ACCESS TO  
UNAUTHORIZED SATELLITE COMMUNICATIONS UNDER THE FEDERAL  
COMMUNICATIONS ACT**

**(AGAINST INFOMIR DEFENDANTS)**

216. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

217. 47 U.S.C. § 605(e)(4) prohibits, inter alia, manufacture and distribution of an electronic or mechanical device which is primarily of assistance in the unauthorized decryption of satellite cable programming.

218. Infomir Defendants are engaging in behavior prohibited by 47 U.S.C. § 605(e)(4) by their manufacture (or other prohibited activity) with respect to the set-top boxes. The set-top boxes are a “device or equipment” that the Infomir Defendants know or should know is “primarily of assistance in the authorized decryption of satellite cable programming” because Infomir controls access to the set-top boxes through firmware and Stalker Middleware and permits infringers to use the set-top boxes.

219. With respect to damages under the Federal Communications Act, 47 USC §605(e)(4), the FCA provides the election between a special measure of actual damages and statutory damages. Broadcasters reserve the right to elect statutory damages as provided for under 47 USC §605(e)(3)(C) *et seq*, namely, to seek \$10,000 to \$100,000 from Defendants as a result of each occurrence.

**COUNT THREE**

**UNAUTHORIZED INTERCEPTION, RECEPTION, AND ASSISTANCE IN  
INTERCEPTING OR RECEIVING BROADCASTS IN VIOLATION OF 47 U.S.C. § 553**

**(AGAINST ALL DEFENDANTS)**

220. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

221. Broadcasters allege this Count Three in the alternative to Count One.

222. Broadcasters own the rights to, among other things, broadcast, re-broadcast, market and distribute within the United States and elsewhere their encrypted programs which are currently de-encrypted and/or distributed through the websites and software distributed by Defendants.

223. 47 U.S.C. § 553 prohibits any unauthorized party from intercepting or receiving, or assisting in intercepting or receiving any communications service offered over a cable system.

224. Assisting in intercepting or receiving under 47 U.S.C. § 553 includes “the manufacture or distribution of equipment intended by the manufacturer or distributor ... for unauthorized reception” of said communications service.

225. Congress has stated that 47 U.S.C. § 553 is “primarily aimed at preventing the manufacture and distribution of so-called ‘black boxes’ and other unauthorized converters which permit reception of cable service without paying for the service.”

226. Any person aggrieved by a violation of 47 U.S.C. § 553 may bring a civil action in a United States district court or in any other court of competent jurisdiction.

227. Defendants have not received a license from any Broadcaster to de-encrypt broadcast or re-broadcast its programs, nor has it received any other permission, express or otherwise, to do so. Through their Websites, Defendants have and continue to intentionally

pirate, retransmit and publish Broadcasters' programs for the sole purpose of their own economic gain and to the detriment of Broadcasters and their licensees.

228. Without the express permission of any Broadcaster or Broadcasters collectively, Defendants are intercepting, receiving, and assisting in intercepting or receiving communications belonging to Broadcasters and causing their contents and substance to be divulged and published through unauthorized channels of transmission or reception.

229. Defendants actions were committed willfully and for purposes of commercial advantage or private financial gain in violation of 47 U.S.C. § 553(c)(3)(B).

230. By reason of the aforementioned conduct, Defendants herein willfully violated 47 U.S.C. §553, thereby giving rise to a private right of action.

231. As a direct and proximate result of Defendants wrongful actions, Broadcasters have sustained and will continue to sustain damages and irreparable harm such that monetary, preliminary and permanent injunctive relief is warranted as authorized by 47 U.S.C. § 553(C)(2).

232. As a result of Defendants' violation of 47 U.S.C. §553, Broadcaster is entitled to damages in an amount, in the discretion of this Court, of up to the maximum amount of statutory penalties, plus the recovery of full costs, interest and reasonable attorney's fees.

233. Without further Discovery from and/or admission by Defendants, Broadcasters cannot determine if Defendants intercepted Broadcasters' signal via a cable system, in violation of 47 U.S.C. §553, or via a satellite transmission, in violation of 47 U.S.C. §605. As such, Broadcasters are alleging two (2) counts in its Complaint. Broadcasters recognize that each Defendant can be liable for only (1) of these statutes.

**COUNT FOUR**

**UNAUTHORIZED DECRYPTION OR CIRCUMVENTION OF  
TECHNOLOGICAL MEASURES IN VIOLATION OF THE DIGITAL MILLENIUM  
COPYRIGHT ACT**

**(AGAINST ALL DEFENDANTS)**

234. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

235. The Copyright Act, as amended by the Digital Millennium Copyright Act (“DMCA”), provides that “[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title.” 17 U.S.C.A. § 1201(a)(1)(A).

236. The DMCA is specifically targeted at the circumvention of digital walls guarding copyrighted material and the trafficking in circumvention tools.

237. The Channels and Programming are subject to the protections of the Copyright Act by virtue of the Berne Convention.

238. The Programming is encrypted by Broadcasters. Only authorized viewers may lawfully access the Programming.

239. The Broadcasters’ encryption is a technological measure which effectively controls access to works protected under the Copyright Act.

240. Defendants are not authorized users. Defendants have descrambled or decrypted or have otherwise bypassed, removed, or deactivated the encryption placed upon the Programming by Broadcasters.

241. Upon information and belief Defendants, or parties working in concert with Defendants, use sophisticated digital recorders to steal Broadcasters signals and de-encrypt the Programming.

242. Defendants' conduct, in circumventing Broadcasters' technological measures, allows unauthorized users to gain access to the work without Broadcasters' permission.

243. Defendants have done so in order to access, market, sell, profit and otherwise benefit from the Programming to the detriment of Broadcasters. Defendants' devices and websites do not have any substantial non-infringing uses.

244. A violation of the anti-circumvention rules under the DMCA is actionable even in the absence of a finding of infringement.

245. Accordingly, Defendants are in violation of the DMCA and Broadcasters are entitled to injunctive relief and damages in an amount to be determined at trial together with any such other and further relief as deemed just, proper and equitable. The Broadcasters reserve the right to elect statutory damages under 17 USC §1203(3)(C)(A).

#### **COUNT FIVE**

#### **TRAFFICKING IN DECRYPTION TECHNOLOGY IN VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT**

#### **(AGAINST ALL DEFENDANTS)**

246. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

247. The DMCA is specifically targeted at the circumvention of digital walls guarding copyrighted material and the trafficking in circumvention tools.

248. The Channels and Programming are subject to the protections of the Copyright Act by virtue of the Berne Convention.

249. The Programming is encrypted by Broadcasters. Only authorized viewers may lawfully access the Programming.

250. The Broadcasters' encryption is a technological measure which effectively controls access to works protected under the Copyright Act.

251. 17 U.S.C. § 1201(a)(2) provides that no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that is designed or produced for the purpose of circumventing a technological measure, or has only limited commercially significant purpose or use other than circumvention, or is marketed by that person or another person acting in concert with them for use in circumvention of such measures.

252. 17 U.S.C. § 1201(b) prohibits the manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that, inter alia, is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

253. Defendants have manufactured, provided, trafficked, or otherwise offered to the public technology, products, and services which have facilitated the circumvention of Broadcasters technological measures.

254. Such trafficking includes but is not limited to the distribution of IPTV players similar to cable boxes which are pre-loaded or capable of loading applications (including Stalker Middleware by the Infomir Defendants and IPTV Players by Streaming Defendants) developed by Defendants or parties in concert with Defendants which permits end-users to bypass Broadcasters' technological measures to view the Programming.

255. Infomir Defendants offer to the public set-top boxes that are either pre-loaded or capable of loading applications that connect directly to Broadcasters Programming (the MAG and AURA boxes, described above).

256. These set-top boxes are primarily designed for the purposes of circumventing the Broadcasters' technological measures controlling access to Broadcasters' copyrighted works.

257. The set-top boxes offered by Infomir Defendants have limited commercially significant purpose or use other than this circumvention.

258. Infomir Defendants market these set-top boxes with the knowledge that they will be used primarily, if not exclusively, for the purpose of circumventing Broadcasters' technological measures.

259. Infomir Defendants collaborate with Teletec (which manufactures the AURA and MAG set-top boxes) and either creates or works with another entity to obtain the Stalker Middleware which is used to effectuate the scheme described above.

260. A violation of the anti-circumvention rules under the DMCA is actionable even in the absence of a finding of infringement. Accordingly, Defendants are in violation of the DMCA and Broadcasters are entitled to injunctive relief, costs, reasonable attorneys' fees and damages in an amount to be determined at trial together with any such other and further relief as deemed just, proper and equitable.

261. The Broadcasters reserve the right to elect statutory damages under 17 USC §1203(3)(C)(A).

## **COUNT SIX**

### **TRADEMARK INFRINGEMENT UNDER § 43 OF THE LANHAM ACT**

#### **(AGAINST ALL DEFENDANTS)**

262. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

263. Broadcasters' marks are protected pursuant to the laws of the Russian Federation and therefore entitled to protection under the Lanham Act by virtue of the Paris Convention.

264. Defendants' use of the Channels' trademarks, including but not limited to the logos, to promote, market or sell products and services on the moidom.tv, mypanorama.tv, gudzon.tv, teleprom.tv, and vdali.tv websites constitutes trademark infringement pursuant to Section 43 of the Lanham Act, 15 U.S.C. § 1125.

265. Defendants' infringement of Broadcasters' trademarks is intentional and willful and has caused and will continue to cause irreparable damage to Broadcasters for which there is no adequate remedy at law.

266. This is an "exceptional case" under the Lanham Act.

267. Accordingly, the Court should grant injunctive relief barring Defendants from intercepting, broadcasting, re-broadcasting or otherwise displaying Broadcasters' Channels and Programming or otherwise infringing upon Broadcasters' marks as well as an award of damages, costs, and reasonable attorneys fees along with any other relief that the Court deems just, proper and equitable.

## **COUNT SEVEN**

### **FALSE ADVERTISING UNDER § 43 OF THE LANHAM ACT**

#### **(AGAINST ALL DEFENDANTS)**

268. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

269. Defendant's advertisements and statements concerning their authority to broadcast the Programming are literally and/or implicitly false, misleading, and in direct violation of Section 43(a) of the Lanham Act, which provides in relevant part that "[a]ny person who, in connection with any goods or services . . . uses in commerce any . . . false or misleading description of fact or misleading representation of fact, which . . . in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her

or another person's goods, services, or commercial activities, shall be liable to a civil action by any person who believes that he or she is likely to be damaged by such act."

270. As set forth in **Exhibits 15-18**, Defendants have misappropriated the logos and other protected marks of Broadcasters' Channels for their own commercial gain and to the detriment of Broadcasters.

271. Pursuant to 15 U.S.C. § 1125, 1117, Broadcasters are entitled to injunctive relief, damages for Defendants' Lanham Act violations, an accounting of profits made by Defendants on revenues relating to the Programming, recovery of costs and reasonable attorney's fees incurred in this action along with any other relief that the Court deems just, proper and equitable.

## **COUNT EIGHT**

### **COPYRIGHT INFRINGEMENT**

#### **(AGAINST ALL DEFENDANTS)**

272. Broadcasters hereby incorporate and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

273. The Berne Convention requires member states, including the United States, to recognize the copyrights issued with respect to works created in other member states.

274. Art. 2 of the Berne Convention provides that the Berne Convention applies to cinematic works.

275. The Programming need not be registered with the United States Copyright Office in order to be eligible for protection under the Copyright Act as applicable here through the Berne Convention.

276. Broadcasters (and/or their parents, subsidiaries, licensees or affiliates) are the legal or beneficial owners of the copyrights in the Channels and Programming that have been or will be distributed via encrypted satellite transmissions to be exhibited over broadcast or internet

television stations in the United States or abroad as well as through a variety of other media outlets.

277. Article 1332 of the Civil Code provides that all broadcasts that originate in the Russian Federation are protected by Russian law.

278. Russian law protects neighboring rights which, as relevant here, are the rights a broadcaster has in its broadcasts including the rights to re-broadcast its broadcasts. *See* Art. 1330.2 of the Civil Code which protects a broadcaster's right to record; reproduce; distribute; and re-transmit its original broadcast.

279. Russian law does not require any formalities, such as registration, for a broadcaster to exercise neighboring rights.

280. Each Program is an original audiovisual work that has been or will be fixed in a tangible medium of expression and constitutes copyrightable subject matter within the meaning of Section 102 of the Copyright Act, 17 U.S.C. § 102.

281. Each Program has been created or licensed for exhibition by Broadcasters (and/or their parents, subsidiaries, licensees or affiliates), the transmissions of which Defendants are broadcasting or re-broadcasting by, among other methods, streaming them over IPTV, without authorization on their websites. Upon information and belief, Defendants have streamed and will continue to stream, as part of their unauthorized service via their websites and/or hardware, the Channels and Programming.

282. Under Section 106 of the Copyright Act, 17 U.S.C. § 106, Broadcasters own the exclusive rights, among others, to reproduce in copies their copyrighted works, to distribute copies to the public of their copyrighted works, to publicly perform their copyrighted works, to publicly display their copyrighted works, and to make derivative works based upon their copyrighted works.

283. Under Section 106 of the Copyright Act, 17 U.S.C. § 106, Broadcasters (and/or their parents, subsidiaries, licensees or affiliates) also own the exclusive right to authorize others to exercise the rights set forth in the preceding paragraph 54.

284. Neither any of Broadcasters nor any other person or entity authorized by Broadcasters has granted any license, permission or authorization to Defendants to exercise any of the rights as set forth in this Complaint or to authorize others to exercise such rights with respect to the copyrighted Programs or any other works in which Broadcasters (and/or their parents, subsidiaries, licensees or affiliates) own copyrights.

285. In offering their infringing services, Defendants have exercised and will exercise (or has authorized or will authorize others to exercise) one or more of Broadcasters' exclusive rights set forth in this Complaint with respect to the Programming and other works in which Broadcasters (and/or their parents, subsidiaries, licensees or affiliates) own copyrights.

286. Defendants have committed and will continue to commit each act of copyright infringement with the knowledge that it was not authorized to exercise any of the rights (or to authorize others to exercise any of the rights) set forth in this Complaint with respect to the Programming and other works in which Broadcasters own copyrights. Defendant's conduct thus has constituted and will constitute willful copyright infringement.

287. By facilitating and aiding these infringements, John Does are contributing to copyright infringements and are thus vicariously liable under the Copyright Act 17.U.S.C. §101 et seq.

288. As a result of Defendants willful copyright infringement, Broadcasters have been and are being irreparably harmed.

289. The Copyright Act provides for, among other things, injunctive and monetary relief to remedy such instances of infringement. 17 U.S.C. §§ 502, 504.

290. Unless restrained by the Court, Defendant will continue to engage in such willful copyright infringement.

291. Accordingly, the Court should grant injunctive relief barring Defendants from intercepting, copying, broadcasting, re-broadcasting or otherwise displaying the Channels and Programming as well as an award of damages along with any other relief that the Court deems just, proper and equitable.

## **COUNT NINE**

### **SECONDARY COPYRIGHT INFRINGEMENT**

#### **(AGAINST ALL DEFENDANTS)**

292. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

293. Federal common law imposes secondary liability on a party that has not directly infringed a copyright, but has played a significant role in direct infringement committed by others by, for instance, providing direct infringers with a product that enables infringement.

294. Those who distribute infringement-enabling products or services may facilitate direct infringement on a massive scale, making it impossible to enforce copyright protection effectively against each individual John Doe infringer.

295. This count is being pleaded in the alternative and in addition to direct copyright infringement.

296. Infomir Defendants sell set-top boxes with the primary purpose of the decryption of satellite programming. These set-top boxes are marketed, along with the Stalker Middleware and MAGic Solution, to allow infringers to become their own cable company. Infomir Defendants attend trade shows, provide components, and provide training so induce and facilitate such infringement.

297. Through the creation, maintenance and operation of their unauthorized Websites and providing streaming services and credit card processing for [www.mypanorama.tv](http://www.mypanorama.tv), [www.gudzon.tv](http://www.gudzon.tv), <https://moidom.tv/>, <https://vdali.tv>, and <http://teleprom.tv>, Streaming Defendants induce, contribute to, and are vicariously liable for any copyright infringement committed by their subscribers or other persons that are provided access to the Defendants' infringing services.

298. Accordingly, all Defendants are involved in the interception, decryption, or retransmission of broadcasts which they know to be intercepted or wrongfully decrypted.

299. Defendants conduct is purposeful and actively encourages such infringement. Through these acts, Defendants induce and profit from copyright infringement.

300. Defendants also vicariously infringe upon Broadcasters copyrights through their failure to supervise the activity taking place on their platforms. Infomir Defendants and Streaming Defendants maintain control over the manner in which their products are used and have declined to exercise the right and ability to supervise or control infringing activities.

301. Defendants enjoy a direct financial benefit from the infringements that they contribute to, allow, and induct.

302. Accordingly, the Court should grant monetary damages, costs and injunctive relief along with any such other relief the Court deems just, proper, and equitable.

## **COUNT TEN**

### **NEW YORK GEN. BUS. LAW § 349**

#### **(AGAINST ALL DEFENDANTS)**

303. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs 1 as if fully set forth herein.

304. New York General Business Law § 349 prohibits “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service...”

305. Subsection (h) of General Business Law § 349 provides that “any person who has been injured by reason of any violation of this section may bring an action . . . to enjoin such unlawful act or practice . . .” in addition to the right to recover “actual damages.”

306. Defendants have, through their Websites, deceived consumers and paying customers in New York into believing it has the legal right or authority to broadcast or re-broadcast Programs over which Broadcasters have exclusive rights. The Websites are misleading in a material way by representing that the services to be provided are authorized despite the infringements set forth above. Broadcasters have suffered and continue to suffer irreparable injury as a result of Defendants’ conduct, including their interception, broadcast and re-broadcast of the Programming. Such injuries are not limited to financial injury and include damage to Broadcasters’ worldwide reputations, goodwill and relationships with licensees, among others.

307. Accordingly, Broadcasters are entitled to injunctive relief against Defendants as well as all actual damages caused by Defendants conduct under Gen. Bus. Law § 349 any such other relief the Court deems just, proper and equitable.

#### **COUNT ELEVEN**

#### **UNFAIR COMPETITION AND COMMON LAW INFRINGEMENT (ACCOUNTING)**

#### **(AGAINST ALL DEFENDANTS)**

308. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

309. The conduct of Defendants constitutes unlawful, unfair, and fraudulent business practices in violation of the general business, trade regulation, and unfair competition laws of the State of New York.

310. Broadcasters are therefore entitled to injunctive relief against the injury Defendants have caused to Broadcasters by misappropriation of the Channels, Programming, trademarks are other rights belonging to the Broadcasters.

311. Defendants' wrongful acts have proximately caused and will continue to cause Broadcasters substantial injury, including loss of customers and advertising, confusion of existing and potential customers, injury to their reputations, and diminution of the value of the Programming and of all the works which Broadcasters create and market. The direct damages, lost profits, and other losses sustained by Broadcasters due to Defendants' unlawful conduct are substantial.

312. Broadcasters are therefore entitled to a full and accurate accounting of all the profits the Defendant has obtained as a result of its unfair competition practices with respect to the Programming.

313. Broadcasters are also entitled to an injunction, under principles of equity, restraining Defendants and their officers, agents, servants, employees, and all persons acting in active concert or privity with them from engaging in any further such unlawful conduct along with any such other relief the Court deems just, proper and equitable.

## **COUNT TWELVE**

### **DECLARATORY JUDGMENT**

#### **(AGAINST ALL DEFENDANTS)**

314. Broadcasters hereby re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

315. A case of actual controversy exists regarding Defendants' broadcasts or re-broadcasts of Broadcasters' Channels and Programming that would be resolved through declarative relief from this Court.

316. Therefore, a judgment declaring Broadcasters' exclusive rights to distribute the Programming and Channels in the United States is warranted pursuant to the Declaratory Judgment Act 28 U.S.C. § 2201, *et. seq.*

### **PRAYER FOR RELIEF**

WHEREFORE, Broadcasters request that the Court enter judgment in their favor and against Defendants as follows:

A. A declaration adjudging that Broadcasters own all rights, titles and interests to the Channels and Programming and that Defendants have no rights, title or interest to the Channels and programming;

B. An order permanently enjoining Defendants and their officers, agents, servants, and employees and all those in active concert or participation with them, including but not limited to payment processors, from infringing upon Broadcasters' exclusive rights to the Channels and Programming;

C. An order permanently enjoining Defendants from importing marketing or selling any device that is designed or utilized for the purposes of unlawfully accessing Broadcasters' Channels and Programming

D. Pending the outcome of this litigation, an order permanently disabling the Defendants' Websites and IP addresses used by Defendants, either directly or through the appropriate domain registrar and a registry hold rendering such Websites and IP addresses nontransferable;

- E. A judgment awarding ownership of the Websites to the Broadcasters;
- F. An award to Broadcasters of monetary damages, including, where applicable, statutory damages, costs, together with reasonable attorneys' fees and prejudgment interest;
- G. An award to Broadcasters of exemplary damages;
- H. An award of any such other and further relief as the Court deems just, proper and equitable.

Dated: New York, New York  
April 4, 2017

DUNNINGTON, BARTHOLOW & MILLER LLP  
*Attorneys for Broadcasters*

By: /s Raymond J. Dowd  
Raymond J. Dowd  
Samuel A. Blaustein  
250 Park Avenue, Suite 1103  
New York, New York 10177  
(212) 682-8811  
rdowd@dunnington.com  
sblaustein@dunnington.com